
Article:
Marshall, Angus M. and Paige, Richard orcid.org/0000-0002-1978-9852 (2018) Requirements in digital forensics method definition : Observations from a UK study. Digital Investigation. ISSN 1742-2876

https://doi.org/10.1016/j.diin.2018.09.004

Requirements in digital forensics method definition: observations from a UK study

Angus M. Marshall, Richard Paige

Dept. of Computer Science, University of York, UK

Abstract

During a project to examine the potential usefulness of evidence of tool verification as part of method validation for ISO 17025 accreditation, the authors have examined requirements statements in several digital forensic method descriptions and tools. They have identified that there is an absence of clear requirements statements in the methods and a reluctance or inability to disclose requirements on the part of tool producers. This leads to a break in evidence of correctness for both tools and methods, resulting in incomplete validation. They compare the digital forensics situation with other ISO 17025 accredited organisations, both forensic and non-forensic, and propose a means to close the gap and improve validation. They also review existing projects which may assist with their proposed solution.

Keywords: ISO 17025, ISO 27041, quality standards, method validation, Tool verification, forensic tool development

1. Introduction

ISO/IEC 27041 [1], as part of a group of standards dealing with digital investigations, is the standard which describes a process by which a method can be shown to be fit for its intended purpose. To achieve this, it proposes a process for the validation of methods used in a digital investigation. Within the description of validation it suggests that evidence of a tool's verification against a declared set of requirements can be used as means to reduce the amount of validation required for processes in which the tool participates.

Email address: angus.marshall@york.ac.uk (Angus M. Marshall)

This work was supported by the University of York Research Priming Fund

i.e. it suggests that those process requirements which are wholly satisfied by the tool, and for which evidence of verification exists, need not be subjected to further testing.

Note: in this project we have concentrated solely on the validation and verification issue. The other standards in the group propose models of evidence gathering and processing which. although useful, are not considered core issues for this work.

From the perspective of software engineering the proposal in ISO/IEC 27041 [1] is entirely acceptable. However, for such a mechanism to succeed, the tool and the process in which it participates must be specified in terms of requirements which can be mapped against each other to show how the tool conforms to, or partially fulfills, the requirements of the process.

In effect, the proposal is that there is some degree of overlap between tool requirements and method requirements, ranging from the possibility that a tool's requirements are a complete subset of a method's requirements (Figure 1) to the, potentially, less likely situation where a method's requirements are a subset of a tool's (Figure 1).

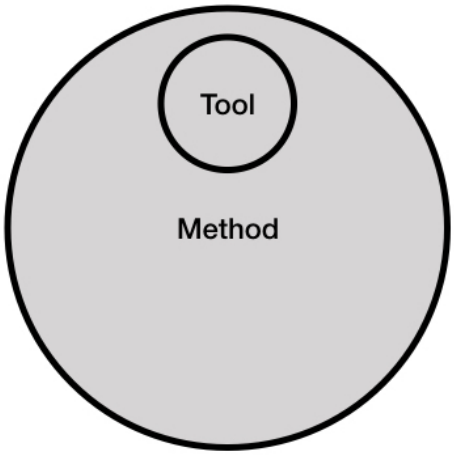

Figure 1: Tool requirements are a subset of method. Typical of specialist tools or small tools produced to assist with part of a method.(Shaded area = the set of requirements which much be satisfied for validation.)

In practice, because some of the requirements for a method with an investigative context will be non-technical in nature, it is believed that the most common situation will be that shown in Figure 1, where a tool's requirements

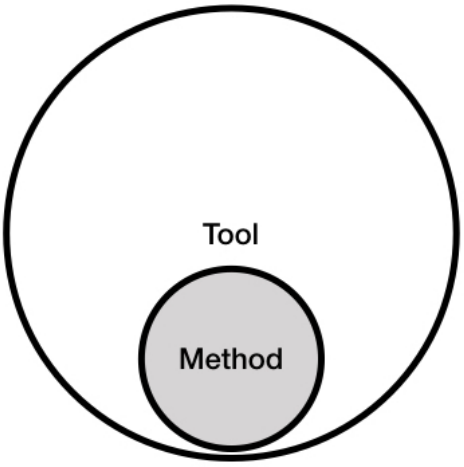

Figure 2: Method requirements are a subset of tool. Considered rare, but possible where a method exactly follows a process defined by the tool producer and uses only a subset of the tool functionality.(Shaded area = the set of requirements which much be satisfied for validation.)

intersect with those of a method, and only those tool requirements lying in the intersection are relevant to the validation of the method.

During research into how this mechanism could be applied in practice, particularly to allow producers of tools for digital forensic processes to support their customers' compliance with ISO 17025's[2] validation requirement [2], through disclosure of evidence of testing and without compromising commercially sensitive information such as details of test data, the authors have found that such a mapping appears, at the time of writing, to be impossible to perform. This is because it has proved impossible to obtain the necessary levels of information about requirements from any of the participants in the study. Two main factors appear to affect this:

- Firstly, the process definitions examined in our study do not contain any technical requirements which can be mapped. Rather, they contain primarily non-technical requirements aligned to the needs of the

[2]In this document we concentrate on the use of ISO 17025:2005 as the currently deployed standard. We consider the implications of transition/update to the 2017 version in the Conclusions of this document

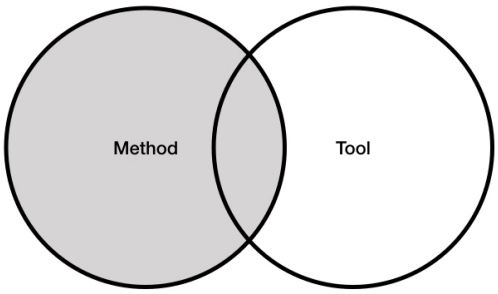

Figure 3: Tool requirements intersect with the method. Common where the tool fulfils some or all of the technical requirements, but there are other non-technical requirements to be satisfied.(Shaded area = the set of requirements which much be satisfied for validation.)

Criminal Justice System.

- Secondly, the tool producers are either unable (in the case of most small providers) or unwilling (in the case of most larger providers) to provide information about how they capture customer requirements, let alone disclose what those requirements are.

  Some even went as far as responding to the request for information with statements such as "The information you seek is commercially sensitive as we operate in a very competitive landscape. Unfortunately, we can't give out any specifics on our product development techniques to third parties." The authors struggle to understand this type of response as our questions related to high-level development models and requirements capture methods rather than specific details of implementation of tools or tests. We can only surmise that the tool providers who responded in this way either lack confidence in their own products or believe that they are using innovative development techniques which no other developer has considered.

2. Principles of ISO 17025

Before examining the concept of validation more closely, it may be helpful to review some of the principles which underpin ISO 17025 which are embodied in the earlier version and which have influence its use in "non-forensic"

organisation such as those carrying out calbration of tools or testing of chemical compounds or metal alloys.

Gravel[3], writing in 2002 about the 1999 version of ISO 17025 described 8 principles which were embodied within the standard as:

Capacity Concept that a laboratory has the resources (people with the required skills and knowledge, the environment with the required facilities and equipment, the quality control, and the procedures) in order to undertake the work and produce competent results.

Exercise of responsibility Concept that persons in the organisation have the authority to execute specific functions within the overall scope of work and that the organisation can demonstrate accountability for the results of the work.

Scientific method Concept that the work carried out by the organisation is based on accepted scientific approaches, preferably consensus-based, and that any deviations from accepted scientific approaches can be substantiated in a manner considered generally acceptable by experts in that field.

Objectivity of results 1. Concept that the results produced within the scope of work of the organisation, are mainly based on measurable or derived quantities.

2. Concept that subjective test results are produced only by persons deemed qualified to do so and that such results are noted as being subjective, or are known by experts in that field of testing to be mainly subjective.

Impartiality of conduct Concept that the pursuit of competent results through the use of generally accepted scientific approaches is the primary and overriding influence on the work of persons executing tests - all other influences being considered secondary and not permitted to take precedence.

Traceability of measurement 1. Concept that the results produced, within the scope of work of the laboratory, are based on a recognised system of measurement that derives from accepted, known quantities (SI system) or other intrinsic or well-characterised devices or quantities.

2. Concept that the chain of comparison of measurement between these accepted, known quantities or intrinsic devices or quantities, and the device providing the objective result, is unbroken for the transfer of measurement characteristics, including uncertainty, for the whole of the measurement chain.

Repeatability of test Concept that the test which produced the objective results, will produce the same results, within accepted deviations during subsequent testing, and within the constraints of using the same procedures, equipment and persons used during a previous execution of the test.

Transparency of process Concept that the processes existent within the laboratory producing the objective results, are open to internal and external scrutiny, so that factors which may adversely affect the laboratory's pursuit of objective results based on scientific method, can be readily identified and mitigated.

With the exceptions of Capacity and Exercise of responsibility, these principles establish a need to show, not just that a chosen method satisfies requirements for an intended use, but that the method is fundamentally correct or sound, and satisfies broader ranging technical requirements.

From our reviews of both the 2005 and 2017 versions of ISO 17025, it appears that these principles have been retained in the most recent versions of the standard.

3. Application of ISO 17025:2005 to "non-forensic" disciplines

A regularly voiced criticism of ISO 17025 is that it is, as its title suggests, intended for Testing and Calibration laboratories. In order to understand how ISO 17025 is applied in these "non-forensic" organisations, and to determine if or how it is applied differently in a forensic context, the authors carried out a review of publicly available accreditation records.

The United Kingdom Accreditation Service (UKAS) maintains a register of accredited bodies [4] which is open for public inspection. The entries in this register include detail of each test for which a body has been accredited, giving a brief description of the method used where appropriate or necessary.

Examination of a sample of 100 accredited organisations in a range of "non-forensic" and "non-medical" areas reveals that these organisations apply two approaches to defining the requirements for their accredited process:

Physical properties Where precise measurement of physical properties is possible (e.g. for volumetric, force, torque, acoustics), the schedules of accreditations specify, using SI units, the range of measurement possible and tolerances (uncertainty) allowed for that measurement.

External standards In other circumstances, where an industry has defined its own standards, the accreditation is based on implementation of the published standard which either defines the range and uncertainty for the measurement, or defines the method itself.

In both of these cases, the requirements for the method, and thus its validation, are available in published form (either directly in the schedule of accreditation or in the published standard) and thus can be subjected to independent scrutiny and adopted by others practicing in the same technical field. In fact, the published requirements allow an independent verification of the method to show correctness in the form of conformance to a general set of standardised requirements rather than just conformance to the requirements for a particular use-case.

Moreover, the presence of these published criteria allow customers to identify those testing bodies whose methods may satisfy their needs before entering into discussions with the testing body. In effect, the listed requirements and associated tests become a menu from which the customer and test body can choose the most appropriate way of meeting the customer's particular needs.

4. A Discussion of Validation

In many discussions of accreditation against the standard, the concept of "validation of the tool" or even "tool accreditation" is raised by users and vendors as a means to shortening or eliminating the process. To the authors, this hints that there may be some either confusion about the meanings of these terms, or a different use of language in effect. It is, therefore, instructive to consider the software engineering distinction between verification and validation and contrast it with the ISO 17025 view.

4.1. ISO 17025:2005 approach to validation.

ISO 17025:2005 [2] contains no direct definition of validation but, in accordance with ISO practice, refers the reader to ISO 17000 and ISO 9000 for inheritance of relevant definitions. This practice, of relying on definitions found in other standards, is common with the ISO range of standards, but can cause problems for some users as they may perceive a requirement to have access to the defining standard as well as the standard they are trying to implement, or they may rely solely on common usage of the word as opposed to ISO's stipulative definitions (aka the "Humpty Dumpty" rule[3]). In practice, ISO provides an Online Browsing Platform [6] (OBP) which allows access to definitions and some other text without further expenditure.

Using the OBP, the authors have found that ISO 17000 contains no definition of validation. Thus the ISO 9000:2005 [7] definition should be used as this is the most recently published version prior to the publication of ISO 17025:2005. This gives the following definition of validation:

> Confirmation, through the provision of objective evidence, that requirements for a specific intended use or application have been fulfilled.
>
> NOTE 1 The term validated is used to designate the corresponding status.
>
> NOTE 2 The use conditions for validation can be real or simulated.

and defines objective evidence as

> Data supporting the existence or verity of something
>
> NOTE: Objective evidence may be obtained through observation, measurement, test, or other means.

with requirement as

> need or expectation that is stated, generally implied or obligatory
>
> Note 1 to entry: Generally implied means that it is custom or common practice for the organization (3.3.1), its customers

[3] "When I use a word, it means it means just what I choose it to mean"[5]

(3.3.5) and other interested parties (3.3.7), that the need or expectation under consideration is implied.

Note 2 to entry: A qualifier can be used to denote a specific type of requirement , e.g. product requirement , quality management requirement , customer requirement .

Note 3 to entry: A specified requirement is one that is stated, for example in a document (3.7.2).

Note 4 to entry: Requirements can be generated by different interested parties (3.3.7).

Note 5 to entry: This definition differs from that provided in 3.12.1 of ISO/IEC Directives, Part 2:2004. 3.12.1 requirement expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted

This suggests that validation is a demonstration of suitability for a particular use-case, that the requirements for a validated process should be derived from the intended use-case and that validation should be the process of obtaining data which shows that a method or process meets those specific requirements.

4.2. Software Engineering approach to verification and validation

In the world of digital forensics we tend to rely on third-party tools which we trust have been produced in accordance with good engineering practices. For the most common analytical tools, this is software which we trust has been correctly specified, implemented and tested. However, the responses to our questions about development models suggest that there is some disconnect between the tool producers and the way end-users are expected to provide evidence of fitness for purpose. In order to understand how this may have arisen, we turned to a consideration of Software Engineering terminology to discover if there is a fundamental conceptual difference.

In Software Engineering, we commonly paraphrase Verification as "are we building the product right?" and validation as "are we building the right product?"[8]. i.e. verification is a demonstration of the correctness of the product whereas validation is a demonstration of suitability for a particular use. More formally the IEEE Standard Glossary of Software Engineering Terminology[9],states these as

Verification

> (1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase.
>
> (2) Formal proof of program correctness.

Validation

> The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

For completeness, [9] also defines a requirement as

> (1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents.
>
> (3) A documented representation of a condition or capability as in (1) or (2).

These definitions are completely consistent with those found in the ISO and ISO/IEC standards under consideration.

Software products should, therefore, be subjected to verification during development - to show that they are correct and complete, and validation post-development to show that they meet the requirements for their intended use-cases. In more common terms, the validation test can be considered to be an acceptance test.

In the case of custom software, produced in response to a particular problem, the process of verification could result in validation for that problem. In the case of off the shelf software (e.g. word processors, spreadsheets, common forensic tools), however, verification during the development phases is based on a generic statement of requirements which meets the needs of a perceived customer or a group of idealised customers. It is the responsibility of the customer to ensure that the verified tool provides a valid solution to their problem as part of the procurement and pre-deployment process.

It is, thus, entirely possible to verify a product which cannot be validated as it does not provide a suitable solution to the problem under consideration (e.g. a custom-built spreadsheet may be completely correctly built but

unusable as a presentation package) and it is also possible to validate an unverified product by showing that, despite its inherent flaws, the product satisfies a particular case-specific set of requirements. For example, a calculator which always states that 2+2=5 is unlikely to be verifiable, but can participate in a validated method where the requirement is to calculate that 3+3=6. Similarly a tool, designed to parse FAT filesystems only, will not parse NTFS. It is therefore, not verifiable for NTFS but can participate in methods which are validated for examination of a FAT formatted filesystem.

In the latter case the unverified product cannot be shown to have any utility beyond the limited circumstances for which it is validated.

In the former case, however, the verified product may be useful in other situations and the presence of evidence of verification can be used to assist the process of choosing it as a potential solution - i.e. the evidence of verification may show that the validation requirements have already been met during the development process.

This depends entirely on the existence of suitable statements of requirements for both the tool as it was developed and the situation in which it is to be used, and satisfactory evidence that those requirements have been satisfied.

4.3. Implications for method validation

Given that the definitions and usage of validation and verification, as outlined above, appear to be consistent it should, therefore, be possible to use software engineering evidence of verification, as suggested in ISO/IEC 27041 [1] as part of the validation of a suitably documented method.

5. Our study

5.1. Laboratory documentation

In our study, we examined a small randomly chosen set of Standard Operating Procedures (SOPs) and Validation plans and records from two accredited digital forensic laboratories. The SOPs were written in a format which appears to be based on the SWGDE Model [10] and be consistent with the accepted standard format within forensic science laboratories in the UK. These contain sections detailing Purpose, Scope, Equipment, Limitations, Procedure, Processing, Success/Failure Criteria and References. None of these SOPs contained any obvious definitions of technical requirements. Rather they tend to define success in terms of processing completing without

any errors being reported, and give a broad area of application in the Scope statement.

Validation plans contained some identified requirements, but these were arranged as End User (the Criminal Justice System), Legal (including compliance with ISO 17025), Compatibility (output format only) and Ethical. No obvious low-level technical requirements were specified in any of the plans.

Validation records showed that validation processes tended to consist of evidence that the process under test produced the same results as the same process run on other equipment or that it produced expected results from a particular test case.

The testing thus satisfied the letter of the ISO 17025:2005 description of validation, but may not have achieved the level suggested by the principles in [3], particularly in respect of Traceability and Transparency.

This apparent failing is not thought to be a problem for other forensic disciplines whose roots lie in other sciences such as chemistry, physics or biology, where the methods used in forensic laboratories are specific adaptations of well-known methods which are used for other purposes and which have been subjected to rigorous peer-review through publication and extensive use in other work.

Digital Forensics, however, has its roots in engineering and is highly reliant on reverse-engineering of decisions and implementations made by others. Many of these implementations (e.g. hard disc firmware, filesystem implementations, data caching) are not published or reviewed as they are commercially sensitive and/or there is no need for the majority of users/customers to have any particular interest in the low-level implementational detail which is of particular interest to a digital forensic examiner or analyst. As a result, it may be considered to be difficult for producers or users of forensic tools to show that the tools are actually correct except by potentially lengthy and costly empirical methods.

This is compounded by a fundamental difference in the nature of the way in which off the shelf software (OTSS) is used. In a non-forensic context, OTSS is typically intended to process inputs provided by a user in order to generate a particular output. In this situation, the inputs are known, or can be examined, before the output is seen and thus detection of incorrect results can be simple. In the forensic context, however, examinations start with a source of potential evidence whose contents are unknown. Thus the inputs to the whole forensic process are unknown. Although the user may have some experience of what abnormal outputs look like, this depends entirely

on the tool actually producing abnormal outputs or indications of errors. It is entirely possible for a tool to process inputs incorrectly and produce something which still appears to be consistent with correct operation. In the absence of objective verification evidence, assessment of the correctness, or otherwise, of any results produced by a tool relies solely on the experience of the operator.

It should also be borne in mind that updates to hardware and software may have no apparent effect on system behaviour as far as a typical user is concerned, but may dramatically change the way in which internal processing is carried out and data is stored. This impacts both on the ability to recover and interpret data and on the behaviour of the tools used to perform these operations.

5.2. Vendor evidence of verification

Our study circulated a questionnaire and received 14 responses from tool providers. Of these, 2 could be considered major providers although one is more focussed on e-Discovery than criminal investigations.

The 12 small providers seemed confused about what was meant by customer requirements with responses including "I'm my own customer", "Sorry, I don't understand the question', "Forums, social media", "I do not - many potential customers seem utterly bemused why they should be interested at all". Of the 14, 3 identified the use of JIRA / Confluence /Github as a means of deriving requirements and three others identified Meetings and Communications with end users as the mechanisms used.

When asked how they demonstrated that their tool satisfied user requirements, responses include use of NIST test disc images, use within ISO 17025 accredited laboratories, and meetings. Only one of the survey group mentioned compliance testing.

We also, as noted in the introduction, met with considerable resistance from some of the better-known providers when we asked for information about this topic. As a result, we cannot provide objective evidence for any degree of confidence that tool providers are meeting the genuine requirements of the digital forensic laboratories.

Customers for the tools have little incentive to consider the technical requirements as it seems possible to obtain accreditation to ISO 17025:2005 without them, and most tool providers are either unable or unwilling to provide evidence that they have verified their tools against any customer or technical requirements.

6. Transition to ISO 17025:2017

The position in respect of accreditation to ISO 17025:2017[11] may be somewhat different as this now contains definitions of validation and verification which are very similar to those used in ISO 27041 and the software engineering world, viz:

Validation Verification, where the specified requirements are fit for an intended use

Verification Provision of objective evidence that a given item fulfils specified requirements

Thus validation appears, in the newer version, to be reliant on verification against specified requirements and comparison of those requirements with the requirements of the intended use-case.

7. Conclusion

Contrary to previous arguments that ISO 17025 [12] is an unwieldy standard for digital forensics because of the complexity of validation, we believe that it can be applied if certain preconditions are met.

For ISO 17025 to be successfully applied, the existing understanding of requirements needs to be reconsidered. Rather than relying on the concepts of "customer requirements" [13], where the customer is the customer of the laboratory (i.e. law enforcement agents, lawyers, the criminal justice system etc.) to provide the baseline for method validation, forensic science providers should consider the *technical requirements for their own processes and use the* customer requirements as a means of selecting the most appropriate processes to deploy. This would be consistent with the way other "non-forensic" accredited testing and calibration organisations operate.

Within forensic science disciplines we suggest that all labs. will have the same common core technical requirements for generic method types (e.g. in digital forensics, hard disc imaging is a core process, as is extraction of data from devices running specific iOS versions etc.), that these should be established by technical working groups from within each discipline, and documented in agreed international standards which can be maintained for use and development by the community.

The requirements contained in these standards can then form the basis of a specification mechanism for methods. Clear identification of the technical requirements vs. the non-technical would allow producers and users to identify priority areas for new tool development.

Publication, and public maintenance, of this common set of requirements would also allow transparency in the verification and validation process. Rather than relying on "commercially sensitive" information, which may or may not be correct, it would become possible for all those involved to use the disclosed information and make claims (with appropriate substantiating evidence) based upon it.

Furthermore, if the suggestion of ISO/IEC 27041:2015 [1] that processes should be designed to be atomic in nature (i.e. small, single purpose with low coupling and high cohesion to other processes) can be followed, the set of requirements for any one process can be kept to a minimum, resulting in a better defined set of conditions for validation and an elimination of revalidation being triggered by changes elsewhere in the process. All the methods which were volunteered for our study were monolithic in nature and contained a high degree of repetition of tightly coupled (by virtue of being included in each SOP) initial process stages (e.g. retrieval of physical items from an evidence store) before progressing to the unique elements of the process.

8. Existing related work

8.1. Introduction

Since starting the original project, we have been made aware of some projects which may provide, at least in part, some of the missing requirements, specifications and evidence of correctness. A brief review of two of these, in the context of our analysis and proposals, is given below.

8.2. NIST/DHS Computer Forensics Tool Testing

The National Institute for Science and Technology (NIST) and the Dept. of Homeland Security (DHS) have started some of this work in their Computer Forensics Tool Testing programme [14] (CFTT). In this project, a steering group defines the requirements for particular tool functions and NIST then tests tools against the resulting specifications. At the time of writing, the coverage is somewhat limited, concentrating on a few areas which may

be particularly common in investigations, but a good range of tools has been considered and an online catalogue of tools and results has been produced.

The Federated Tool Testing project as a sub-project of this initiative may be a particularly useful model as it makes available a test suite which can be used by anyone who wishes to test tools against the requirements already defined by the project and share their results.

It is unclear, however, how the programme's priority areas are established or how the requirements are, themselves, validated at as this part of the process does not appear to be documented. It is also noteworthy that the requirements are purely at the tool level rather than the broader method level. This may result in an undue emphasis on producing requirements for existing tools, at the expense of producing requirements which have not yet been satisfied but which should be considered high priority as they reflect an emerging real problem area.

We also suggest that a broader consideration could create opportunities for better tool integration (i.e. improved exchange of data between tools and better cohesion for improved process flows) as well as improved concordance with external requirements such as legal issues.

8.3. SWGDE guidance on testing and validation

The Scientific Working Group on Digital Evidence (SWGDE) has issued a number of documents which are intended to assist in the design, implementation and validation of methods for digital forensic processes. Of these, the two which appear to have most direct application to the area we are investigating are

- SWGDE Recommended Guidelines for Validation Testing [15]
- SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics [16] (At the time of writing, this document was in draft form and had been issued for consultation).

The SWGDE validation guidance[15] states that

> Validation testing should be applied to all tools, techniques and procedures

and further that

> Tools, techniques and procedures, which, by virtue of their widespread use, duration of use, and acceptability by the larger information technology community, are generally acknowledged as reliable and trustworthy. Consideration may be given to the general acceptance of a tool, technique, or procedure in the determination of whether validation is required.

. The latter paragraph appears, to some extent, to contradict the former. In our experience, it seems that this is generally interpreted to mean that something which is in widespread use may be considered reliable.

We argue that this is not the intent of the "general acceptance" statement. In part, this is because of the presence of the phrase "larger information technology community" which is a clear indication that the tools, techniques and procedures under consideration are of a more general-purpose nature than the specialist tools deployed in an investigative context. Spreadsheets, word processors, email programs etc. may generally be considered acceptably reliable because they have minimal impact on evidential product and, should they prove to have an error, the sheer number of users worldwide means that it is likely to be detected and documented relatively quickly.

More importantly, however, if this general acceptance principle is allowed to apply to commonly adopted "forensic" tools, techniques and procedures it has the potential to result in bad evidence. If the tool, technique or procedure has not been subjected to independent scrutiny (e.g. through peer-reviewed publication or properly evidenced validation testing) there is insufficient evidence that it does work correctly. As we note above, digital forensics relies heavily on reverse engineering in order to process and interpret data. At the level that most users operate, it does not have sufficient foundational scientific principles to allow a reversion to first principles to be applied in order to demonstrate correctness. There is always likely to be some doubt or uncertainty about the way the data is being processed and interpreted. This can be reduced only through production of evidence of correctness and adequacy through appropriate software engineering methods, such as testing.

Note: we do not see this as a flaw in the SWGDE guidance, but rather in the way that a large part of the community has chosen to interpret this particular recommendation. It should be noted that similar phrases appear in other guidance and, in our experience, are similarly interpreted.

The remainder of this document gives a high-level overview of the development of a testing procedure which, if underpinned by well-defined require-

ments which allow the identification of appropriate test cases could result in good evidence of validation and identification of boundary cases for methods.

The tool testing guide[16] is more detailed in its recommendations and gives advice about specific tool types and the conditions which should be considered for their testing. Again, however, it makes little reference to using a well-defined set of requirements to assist in the identification of test cases. It does acknowledge that the testing proposed is purely a minimum and that organisations should consider their own particular requirements.

It is our view that evidence of testing, produced in the recommended way, could be applied as an adjunct to method validation, providing the requirements are properly defined and documented. It should be remembered, however, that tool testing alone is unlikely to be produce the evidence of validation required by either ISO 17025[2][11] or ISO/IEC 27041[1], unless it can be clearly shown that the method is wholly and solely implemented by the tool (see Figure 1).

9. Final thoughts

While the NIST and SWGDE projects outlined above may start to provide the type of evidence that is necessary to demonstrate that a method is valid, the potential lack of transparency in the requirements definition processes introduces another element of uncertainty. i.e. if the requirements cannot be shown to be correct, can tests based on those requirements show correctness? This can, to a large extent, be addressed by adopting the "non-forensic" accredited organisation model of using publicly available agreed standard specifications/requirements and/or methods which can be subjected to external independent scrutiny.

It also be useful to engage in a more open process, similar to those proposed for use in the specification and testing of safety-critical systems [17].

[1] ISO/IEC, ISO/IEC 27041:2016 guidance on assuring the suitability and adequacy of digital investigation method (2016).

[2] ISO, ISO 17025:2005 general requirements for the competence of testing and calibration laboratories (2005).

[3] J. Gravel, Principles behind the requirements of iso 17025, online at http://www.cala.ca/ISO-IEC_17025_Principals.pdf, 2002. Last accessed 25th April 2018.

[4] UKAS, Directory of accredited organisations, online at https://www.ukas.com/services/other-services/directory-of-accredited-organisations/, 2018. Last viewed 4th June 2018.

[5] Rev. Charles Dodgson (Lewis Carroll), Through the Looking Glass, 1872.

[6] ISO, ISO online browsing platform, online at https://www.iso.org/obp/ui/, 2018. Last accessed 13th August 2018.

[7] ISO, ISO 9000:2005 quality management systems – fundamentals and vocabulary (2005).

[8] B. W. Boehm, Verifying and validating software requirements and design specifications, IEEE Softw. 1 (1984) 75–88.

[9] IEEE, Ieee standard glossary of software engineering terminology, IEEE Std 610.12-1990 (1990) 1–84.

[10] Scientific Working Group on Digital Evidence (SWGDE), SWGDE model standard operation procedures for computer forensics, online at https://www.swgde.org/documents/Current Documents/SWGDE QAM and SOP Manuals/SWGDE Model SOP for Computer Forensics, 2012. Last viewed 5th June 2018.

[11] ISO, ISO 17025:2017 general requirements for the competence of testing and calibration laboratories (2017).

[12] P. Sommer, Accrediting digital forensics - what are the choices?, Digital Investigation (2018).

[13] International Laboratory Accreditation Cooperation, ILAC G19:08/2014 modules in a forensic science process (2014).

[14] National Institute for Science and Technology (NIST), Computer forensics tool testing programme, online at https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt, 2018. Last viewed 13th August 2018.

[15] Scientific Working Group on Digital Evidence (SWGDE), SWGDE Recommended Guidelines for Validation Testing (Version 2.0) (2014). Last accessed 13th August 2018.

[16] Scientific Working Group on Digital Evidence (SWGDE), SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics (2018). Draft Version 1.0 dated 9th July 2018. Last accessed 13th August 2018.

[17] L. E. G. Martins, T. Gorschek, Requirements engineering for safety-critical systems: A systematic literature review, Information and Software Technology 75 (2016) 71 – 89.